PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F — A2

(11) International Publication Number: **WO 00/10068**

(43) International Publication Date: 24 February 2000 (24.02.00)

(21) International Application Number: PCT/US99/18356

(22) International Filing Date: 12 August 1999 (12.08.99)

(30) Priority Data:
09/133,824 13 August 1998 (13.08.98) US

(71)(72) Applicant and Inventor: FUISZ, Richard, C. [US/US]; 14555 Avion at Lakeside, Chantilly, VA 20151 (US).

(74) Agent: BODNER, Gerald, T.; Hoffmann & Baron, LLP, 6900 Jericho Tumpike, Syosset, NY 11791 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: APPARATUS FOR AND METHOD OF ELECTRONIC CURRENCY GENERATION, TRANSFER AND REDEMPTION

(57) Abstract

The present invention is designed to overcome these problems and provide an electronic form of commerce that provides acceptable levels of security while at the same time permitting anonymous electronic transfers of money substitutes. In particular, the present invention comprises a new form of electronic money, new forms of electronic counterfeit protection, a new storage device that may, but which does not have to be, used with this new form of electronic currency, an electronic currency generator and an apparatus for tracking incoming cash reserves.

CT

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

APPARATUS FOR AND METHOD OF ELECTRONIC CURRENCY GENERATION, TRANSFER AND REDEMPTION

I. BACKGROUND OF THE INVENTION

The present invention is directed to an apparatus for, and a method of, digitally transferring electronic currency. Currency substitutes are not new. Present currency substitutes include credit cards, debit cards, checks and traveler's checks. Each of these substitutes requires that a user's identification, as well as other forms of account information, is provided with the transaction. Transferring user account information increases the likelihood of theft and increases the number of theft prevention and fraud detection measures that are required for a a reliable currency substitute.

Internet commerce and personal electric commerce has been hindered by people's reluctance to transmit account information and identification information with each transaction. For example using cash one can walk into a store and purchase an item without the store or anyone knowing the person's name, household address, bank and bank account number. Digital commerce is hindered by its lack of ability to maintain just such anonymous forms of financial transfers while at the same time providing an acceptable guarantee that the currency substitute is legitimate and redeemable.

Prior systems, such as that disclosed in United States Patent 5,757,917 use a complex system of networks, confirmation codes and authorization codes. This system requires that user obtain a cardholder account with the issuing institution. This deprives the

user of maintaining transaction anonymity as the system verifies each transaction against the user's account information. The system thus knows that user 1 purchased a loaf of bread at a bakery that is likewise registered with the system. This system prevents commerce between wired and non-wired individuals. That is electronic commerce is not permitted to flow to users that are not pre-registered with the system.

Other forms of Electronic Currency are set forth in Cybercash's Lesson in Web Survival, New York Times August 10, 1998. The article discloses a Secure Sockets Layer system and a Digital Wallet system. In both systems, user's credit card information is transmitted back and forth. In the Secure Socket Layer system a user provides his credit card number which is encrypted and sent to the merchant. The merchant receives and decrypts the information. The merchant then encrypts and sends data to the credit card company. The credit card company opens the data and charges the user's account. In the Digital Wallet system, the digital wallet contains all of the user's credit card numbers and encrypts one of them. The encrypted credit card is sent to the merchant. The merchant cannot read the credit card number but can read related transactional information. The information is forwarded to the credit card company who decrypts the credit card information and charges the user's account. In both of these systems, the user's credit card information is transferred. The present invention is designed to be used without transferring this infomration.

Moreover, all forms of electronic commerce heretofore proposed are based on a network form of authorization, most notably the internet, that all such transactions occur over it. Although perhaps good in intention, these systems are creating two

societies, those wired with credit card accounts capable of engaging in electronic commerce and those that are not. Any electronic commerce must be usable and accessible by all segments of the society. It must be accessible by an inner city youth selling newspapers just as it must be accessible to a corporate vice-president who is fully wired.

The present invention solves these and other problems. The present invention permits anonymous users to receive an electronic currency substitute without first being registered or otherwise authorized, and transfer the electronic currency without otherwise having account information transferred therewith. A simple storage device is also disclosed that can be used to engage in electronic commerce transactions without being wired into a computer network, for example by our mythical newspaper sales person.

Some of the problems to be overcome include: permitting multiple methods of currency creation; creating freely transferable electronic currency that does not require user identification; preventing user counterfeiting and non-user counterfeiting; and providing a changeable standardized structure electronic currency format.

The present invention is designed to overcome these problems and provide an electronic form of commerce that provides acceptable levels of security while at the same time permitting anonymous electronic transfers of money substitutes. In particular, the present invention comprises a new form of electronic money, new forms of electronic counterfeit protection, a new storage device that may, but which does not have to be,

used with this new form of electronic currency, an electronic currency generator and an apparatus for tracking incoming cash reserves.

With these and other objectives, advantages and features of the invention that may become apparent, the nature of the invention may be more clearly understood by reference to the following detailed description of the invention, the appended claims, and to the several drawings attached herein.

II. DRAWINGS

Figure 1 is a schematic diagram of an Electronic Currency Unit (ECU);

Figure 2 is a flow chart for issuing ECU;

Figure 3 is a schematic diagram of ECU structure;

Figure 4 is a flow chart of ECU generation;

Figure 5 is a flow chart of ECU generation;

Figure 6 is a flow chart of ECU generation;

Figure 7 is a schematic diagram of ECU structure;

Figure 8 is a schematic diagram of ECU structure;

Figure 9 is a schematic diagram of an ECU storage device;

Figure 10 is a logic chart for ECU transactions;

Figure 11 is a schematic of an ECU issuing device; and

Figure 12 is a schematic diagram of an ECU network.

III. DETAILED DESCRIPTION OF THE DRAWINGS AND OF THE PREFERRED EMBODIMENT

A detailed description of the invention, including a description of the preferred embodiment, is set forth below.

The present invention comprises several different products and methods that are designed for use alone or in combination with the system described herein. Those of ordinary skill in the art will recognize that these products may be categorized in a number of different ways. For the purposes of this application the following categories will be used: Electronic currency; Storage device; Transaction program; Issuing module; Redemption module; and Network maintenance module.

A. Electronic Currency

The electronic currency unit (ECU) is the basic building block upon which other aspects of the invention are based. Current forms of electronic currency suffer from their inability to be used in a transaction without identifying the parties to the transaction. The present invention solves this problem by using multiple identifiers and encryption techniques.

ECU 1 at its most basic level may consist of a unique algorithm stored on a tangible electronic storage medium 2, a floppy disc at its most basic. A unique algorithm functions as a serial number and a given denomination. When the algorithm that is generated is issued, its value is noted for redemption. Fig 2. An ECU can be issued for

anything of value, including but not limited to U.S. currency, stock, bonds, or tangible or intangible assets. Single algorithm ECU is likely to create storage problems. The length and complexity of the algorithms that are needed will continue to increase the more ECU is used. Although, algorithms are useful as serial number to identify each ECU, their use as a denomination identifier can make transactions difficult. Parties have no way of verifying that an ECU is the denomination claimed without redemption or verification by the issuing institution.

To solve this problem a system of multiple identifiers, which may be algorithms, may be used. A denomination identifier 3 is combined with a serial number identifier 4 . Fig. 3. Denomination identifiers may vary by issuing institution as well as by time. For example rather than provide a currency with a numerical representation of a fixed amount such as $20, the denomination identifier may comprise an algorithm, the length of which may vary, that is recorded as representing $20. The ability to vary denomination identification as a function of serial number and/or time increases security. Denomination correlation tables, which show what amount a denomination identifier corresponds to, may be made publicly available. Fig. 4.

If two different identifiers are used, an encryption algorithm may be applied to one or both. The use of the term encryption refers to standard encryption as well as any formatting of data such that only intended users have access thereto. This permits the electronic currency to be transferred while reducing tampering or changing of the currency. Fig 5. A duel identifier may be used for the denomination, serial number or both.

A two key type system of encryption and decryption is used, such as with a PGP encryption scheme, the safety of the electronic currency may be increased even further. In a two key encryption system, one key is used for encryption and one key is used for decryption. A user can only decrypt an item that has been encrypted with the corresponding encryption key. Access only to the encrypting key does not permit the user to decrypt. Recipients wanting to verify some minimal identifying information about the currency may use publicly available decryption keys to gain access to portions of the encrypted currency showing denomination information. Fig. 12 shows a public verification method. Public verification keys are made available to user over telephone lines or the internet. The user receives the keys and determines the currency's authenticity. A re-encryption key may also be provided. If a re-encryption key is not provided, only a copy of the ECU is decrypted during transaction. Fig.6.

A two-key encryption scheme also assists in preventing tampering by requiring re-encryption after decryption. The re-encryption keys are also publicly available and may change over time. In other words, although multiple public decryption keys may be available to decrypt ECU, only the latest re-encryption key is available. This ensures that all ECU that is re-encrypted is also updated in time. Older keys may be phased out as a function of time, thus encouraging users not to hold ECU for extended periods of time without storing in an authorized institution. Although a counterfeiter may be able to decrypt an ECU and change the denomination, the counterfeiter is unlikely to be able to re-encrypt the currency. Constantly changing re-encryption and decryption keys

will further limit the time period during which a counterfeiter will be able to undermine the currency substitute system and cause damage, if successful.

Multiple duel key encryption permits can also be used, a first level of denomination information to be accessed while not providing access to the entire denomination identifier. Two level duel key encryption permits the lowest level of security to be publicly accessible. Users have access to the public decryption and re-encryption keys. The second level is a secure level that is only to be accessed by the issuing and redemption institution. A third level can also be provided. Issuing institutions may provide designated merchants with access to a decryption and re-encryption key to provide point of purchase verification greater than that available to the public while not giving up ultimate access to the ECU. This merchant-level multiple duel-key encryption form may be provided to the merchants daily, weekly or for each purchase depending on how often the issuing institution changes encryption on new ECU being issued.

1. Electronic Currency Header

Widespread use of ECU can be hampered by requirements for uniformity. If multiple institutions are able to issue ECU and the users are able to freely exchange different types of ECU, the ECU system either has to be of a uniform structure or provision for non-uniform structures must be made.

A preferred option in the ECU is the ability for different institutions to have different ECU structure. To enable this option the ECU is provided with a header 5, a table of contents of the ECU. A standardized header identifies, issuing institution type, the location of information and/or the number or web address to contact for different levels of verification information. Additional information can also be provided.

ECU may vary from issuing institution to issuing institution so long as certain standards are maintained. All ECU must have a value identifier and a denomination, which may be combined or separate. Multiple denomination identifiers may be used but at the very least a single denomination identifier must be present. In addition, the ECU must either contain or be operational with a basic transfer program that at the very least copies an ECU and deletes the original copy.

Different ECU types and formats are made compatible by using a header attached to the ECU, preferably at each level of encryption. The identification header tells the transfer programs where the currency information is contained. For example, the first five bits of the currency header may be used to identify where the basic denomination information is contained, the header may then identify if any program information, such as time dependency, devaluation ability or multi-encryption, information is contained in the ECU and where the data is. A second header 6, encrypted within a second layer 7 of serial identifier or denomination identifiers, may contain information about that level of data as well as the level before it. The second level header may contain selected verification methods, such as the location and value of a string on data in the first level

of data. If the data in the second header does not match that present in the first data, tampering may be present.

Re-organizing ECU structure may be used as yet another basic verification tool or identifier of the merchant or institution that took part in a transaction. The organization of a given ECU may contain information as to the currency's authenticity. For example, a known merchant may interleave denomination and serial number identifiers using a predetermined pattern. These patterns may change over time.

2. Electronic Currency Exchange Rates

As ECU is stored on a storage medium, size of the ECU is an issue. While the level of security for various sized denominations may change, hence changing the relative size of the various denominations, ECU size may still become a factor hampering its everyday use. For example, the security protection for a twenty-five cent denomination may be relatively low. The size may still prohibit a portable holding device from carrying one hundred dollars worth of twenty-five cent denominations. This is acceptable to most, if not all users.

ECU size is more of an issue when change needs to be made or transmitted. One solution to this problem is to have an exchange rate module built into the transaction program, described in detail below. The transaction module will in effect devalue the highest valued ECU by creating multiple identical with exchange rate/devaluation rate information encrypted into the ECU. For example, a hundred dollar denomination

may de devalued through the creation of one hundred identical denominations each containing an encrypted exchange rate of 1/100. It should be noted that all devalued ECUs do not have to be devalued uniformly, non-uniform devaluation is contemplated. For most transactions this method may not be preferred as it provided the increased encryption associated with a one hundred dollar denomination on lower denomination values that otherwise would not be so heavily encrypted. Increased size of devalued ECU may also be purposefully introduced to encourage timely redemption or exchange of all devalued ECU.

It should be noted here however that the denomination algorithm might also include an exchange rate portion for transaction between ECUs base don different currency bases. International exchange of currency is thus easily facilitated.

3. Security Options

Although some security options have been discussed above, additional security options for ECU are available.

Counterfeit prevention used in traditional forms of currency is hampered by time. That is, once currency is released it may not be revoked unless a new currency is issued to replace it. Even then unless all old forms of the currency are rendered void, a period of overlap will exist. Old currency may always resurface. ECU solves this problem by offering a time dependent feature.

ECU may be time dependent, such that it has a life span. In its most crude form, the encryption keys may be phased out rendering ECU useless. For example, each public key may have a life of one month. If ECU is not decrypted and re-encrypted each month, it becomes stale and is rendered useless.

Time dependent ECU may have a short life span of a long life span. ECU may also be generated with a time sensitive program such that the denomination amount is varied as a function of time. This feature provides for interest or other increases in an assets valuation to change automatically as a function of time. Alternately, long living EVU that correspond to stocks or any asset whose value fluctuates may constantly update the value of the ECU base don the latest information provided to the ECU. In this case changes in value may involve an increase in the denomination amount.

ECU may also be embedded in, or contain embedded, programs that are self-executing, such as a time dependent computer virus. A time sensitive program can be attached to or embedded in the ECU that limits the life of the currency, thus requiring the user to periodically store the ECU in an authorized depository that is capable of ECU re-generation or re-issue. Multiple forms of time dependency may be used. The embedded self-executing program may activate after one month has expired in combination with public key time dependency.

Time sensitive currency may be used to force ECU back through the issuing network to gauge its authenticity and the level of counterfeiting and ECU in circulation as a function of assets available for redemption.

The encryption of a self-destruct program or virus may also be used by issuing institutions to guard against counterfeiters.

Institution independence creates a degree of uncertainty that may be used by institutions to periodically vary the basic construction of the ECU and prevent counterfeiting.

In a preferred embodiment the ECU will contain three denomination identifiers and three serial number identifiers. A first layer of two key encryption will be applied to the first denomination and first serial number identifiers. Prior to encryption, additional protection may be obtained by interleaving the two identifiers based on yet another algorithm or pattern. A second denomination and serial number packet is made and attached to the first encryption packet together with a header that identifies the second packet information's location. The header contains a small data string and its location in the first encrypted portion for tamper identification. A duel key encryption is applied to this packet. A third denomination and serial number packet is made and attached to the second encryption packet together with a header that identifies the second packet information's location. This third packet is then encrypted using a single key encryption. A header identifies the issuing institution and denomination information. For basic security, a recipient uses known institutional encryption keys to de-encrypt the ECU and verify its denomination and serial number. For transactions with pre-registered vendors, the second encryption packet may be accessed. The duel key encryption ensures that only authorized vendors with access to both encryption and de-

encryption information access this second packet. Finally, the third packet is provided for institutional use only. The level of encryption may be varied depending on memory constraints.

B. Storage devices

ECU is stored on any form of generally available storage medium, including but not limited to ROM, RAM, DRAM, SRAM, floppy disc or hard drive. Optical storage devices may also be used to reduce inadvertent destruction of ECU by magnetic fluctuations. In essence, any electronic or optical storage medium may be used. If the ECU is not on a storage medium it is in a transfer stage between two storage medium.

Storage medium may come in a variety of forms from ECU on a floppy disc, that is physically transferred, to a portable ECU storage device to an ATM machine equipped to receive and dispense ECU to a hard drive in the issuing institutions operation.

Network storage in accounts or depositories is perhaps the safest form of ECU storage. Network storage may comprise, at its most a basic, a form of electronic safe deposit boxes that are backed up and adequately protected against inadvertent destruction. Network storage can be implemented on a user anonymous basis. Users are allocated disk space to store their ECU. The type and amount of ECU does not need to be determined by the storage device unless some form of disaster insurance is required or the amount of ECU is required to be known for the transaction. Re-encryption for time-dependent ECU can be built in. It is contemplated that the storage networks may

be established to operate automatically, deducting the cost of storage directly from the stored ECU. ECU monitoring can be tied in with the network storage such that the information concerning the existing ECU pool is periodically made known, such as amount, type, issuing institutions, etc.

Fig. 9 shows a typical storage device. The device 8 has an input port 9 that may comprise a bus or infrared electronic transfer signal reception device. A standardized bus is preferable provided that has both male 10 and female bus 11. This permits any two devices to be connected simply by inverting one of the devices. A digital signal processor 12 is connected to the BUS 9 that is in turn connected to a memory device 13 and a power supply 14. Multiple memory devices 13a & 13b may be provided all, or some of which, may be removable. An authorization code memory or public key memory 15, which may be connected to an input device, such as a modem or network, is also provided in memory 13 or as a separate memory. A transaction log memory may also be provided. A processor 16 is also provided and is connected to a digital signal processor, memory and network devices. The device may be designed to be handheld or it may be incorporated into an ATM machine. Devices that are in fixed locations may benefit from dedicated connections to an authorization server that is used to distribute ECU information.

ECU cash registers and electronic currency ATM machines likewise contain similar storage devices. In such cases, the transaction is also tied into traditional forms of currency. The storage medium is thus tied into a processor, which may likewise be tied

into a network through a modem etc. The network connection may be periodic or constant depending on the transactions anticipated and the level of security required.

C. Transactions

Transactions can be carried out in a number of different ways. The level of security required by the users will govern, at least in part, the steps that will be taken. In a basic transaction an ECU will be transferred from one storage unit, say a hand held device, to another. In this case, the two devices are attached. A reversible connector with male and female connectors is ideally provided on all storage devices such that one device may be turned upside down and connected.

The transferring machine designates the ECU to transfer though an input device. Fig. 10. A touch pad or similar input device maybe used. An execution key is then pressed. The receiving device may be placed in the reception mode or the exact amount of ECU being transferred may be input for additional security. The transferring device first sets up a mutual connection with the reception device. If the mutual path is terminated or tampered with during the transfer the transfer is cancelled. A standard communication path is created. The transferring unit searches its memory and locates the ECU to be transferred. This information is transmitted to the receiving device. The receiving device copies the ECU into its memory and erases the original ECU. The transaction is completed. Those of ordinary skill in the art will appreciate that the transfer and erase function can be carried out by either device or a combination of the two of them.

Ideally, the receiving device will transfer the ECU into an authentication memory. The receiving device will perform an initial analysis of the currency header to determine the type of ECU. A search is then initiated of the receiving device's authentication memory to determine if public decryption and re-encryption keys exist. If they do, the authenticity of the ECU can be determined. If the authenticity does not meet a user defined, or predetermined, threshold, the ECU is rejected. The ECU in the authentication memory is deleted and a rejection code is transferred to the transmitting machine. A rejection code is also stored in the receiving device. The rejection codes are stored in a transaction log that sores information relating to identifiers, time, money type, etc., which may be uploaded to the authentication server for processing.

If the ECU is accepted, the receiving device transmits an erase command to the transmitting device to delete the ECU from its memory. A log of the transaction is generated indicating that a currency unit was transmitted and accepted. Both machines may store this log information.

If the transferring unit is unable to identify the correct denomination in its memory, it informs the receiving device of the need for change or devaluation. The receiving unit searches its memory to determine if change can be provided. If a transaction is possible the units proceed in the normal manner. After, receipt and acceptance of the transferring unit's ECU but prior to erasing of the transferring unit's memory, the receiving unit transmits the change. A similar verification process is performed. If both devices accept the transaction, the original ECU is erased from both machines and the transaction is completed.

A similar process may be followed for devalued ECU or use of an exchange rate. It should be noted that increasing value of an ECU is not permitted unless the device is an issuing institution. Exchange rate transactions are carried out in a similar manner. Prior to re-encryption by the receiving machine an exchange rate is inserted into the denomination field and the header is changed accordingly. Upon acceptance of the ECU, the transmitting machine erases the original currency. The receiving machine then transmits copies of the re-encrypted currency to the transmitting device according the exchange rate and transaction amount. Both devices record the change in value in their logs. A copy of the ECU for non-transactional purposes may also be stored and transmitted to the user network. The user network will be described in detail below.

ECU storage devices may also be provided with storage device identifier. The storage device identifiers may be fixed or may be changed each time authentication information is obtained. This identifier may be stored in the transaction log. The authentication key network may download transaction log information and process it for fraudulent activity detection. If an ECU storage device is identified as having been tampered with, and or malfunctioning, the ECU storage device information can be transmitted to all ECU storage devices. During initial contact between two ECU storage devices, malfunctioning devices may be identified and the transaction terminated. This provides yet another level of security and fraud prevention.

The transaction program may also be built into an interactive TV. Alternately, an interactive or home shopping TV program may be use din conjunction with an internet connection or traditional telephone system to provide for ECU transactions.

D. Issuing Device

The issuing device in its most basic form may comprise a computer 17 and a storage device 18. As those of ordinary skill in the art will recognize the computing power necessary to generate more complex encryption may exceed that which is available to the vast majority of home users.

An issuing institution should ideally have the following modules: serial number generation module; denomination generation module; currency generation module; and currency information storage module. Additional modules may include multiple currency and generation modules; encryption modules; program selection modules; currency re-generation modules; tracking module; multi-level authorization module; and asset allocation module.

System security and asset allocation are the two key modules to a successful ECU system. The issuing institution must also be able to redeem the ECU and in that regard must safeguard the assets that it has taken in. The asset may be invested in a variety of commercially available instruments such that the issuing institution may generate supplemental assets. A supplemental assets management module may be operationally connected to the redemption and verification modules. This permits the supplemental

asset management module to periodically predict the amount of funds that either will not be redeemed or will be fraudulently redeemed. Asset allocation permits the supplemental assets to be invested such that the ECU system remains viable.

Issuing institutions may use different currency generation programs so long as its ECU is created according to a given standard. Basic denomination identifiers and transaction routines must be standardized. The level of encryption may vary from institution to institution. In that regard, an institution may chose to use one or multiple algorithms for denomination verification. An issuing institution may chose to attach time sensitive software to each ECU

E. Network

The network 19 is used to provide the public with access 23 to currency information and encryption/decryption keys. The network is also used to collect log information. Any time a storage device 20 contacts the network for updated information the network may require a copy of the storage device's log.

A network monitoring module 21 can be provided that tracks currency usage, including devaluation and rejected transactions. Rejected transactions can also be tracked based on the reason for rejection. For example if adequate change does not exist in the ECU pool, the issuing institutions 22 may be directed to issue multiple lower denomination notes to new user.

It should be noted that because generic public encryption keys are used, users do not need to be identified when connecting their storage devices to the network. Once updated general authentication information is available, user's can engage in transactions anonymously without the transmission of user account information.

With time dependent ECU periodic connection of all storage devices is ensured. The use of new re-encryption keys with the phasing out of old decryption keys will ensure that devices that have not contacted the network in a reasonable amount of time are forced to check in. This periodic connection provides access to a variety of information that can be used to monitor and control the ECU trade. Devices that show a high degree of rejected transactions or other irregular transaction practices may be investigated.

F. Redemption

There are different levels and types of redemption. The transactions discussed above can be though of redemption if a non-ECU is paid for the ECU. Redemption in the context of this disclosure refers to the redemption of ECU to the issuing institution, or its affiliates, and the transfer of non-ECU originally exchanged for the ECU to the presenter. Redemption of ECU involves presenting a ECU to a receiving device that has access to all decryption keys and asset reverses to pay the presenter.

When redeeming ECU a transaction similar to that discussed above may be used. The level of authentication may vary from a full authentication to a partial authentication.

The redemption devices is connected to the asset allocation module, either through as direct connection, network or though periodic updates, to register the redemption of ECU.

ECU that has been redeemed may be re-used, including partial or full re-encrypted.

Those of ordinary skill in the art will recognize the wide commercial applicability of the invention set forth above. Those of ordinary skill in the art will recognize the large commercial use of the electronic currency apparatuses and methods described herein to the banking industry, to the electronic industry and to the internet commerce industry. Those of ordinary skill in the art will recognize that the invention herein described and claimed may be modified and is not limited to the specific embodiments herein described.

We claim:

1. An electronic currency unit comprising:

a storage device comprising a header containing information on the location of a denomination identifier and of a serial number identifier in a digital array, and a denomination identifier and a serial number identifier corresponding to said header information.

2. An electronic currency unit as claimed in claim 1 further comprising:

a second denomination identifier and a second serial number identifier, wherein said second denomination identifier and said second serial number identifier are encrypted with a first encryption.

3. An electronic currency unit as claimed in claim 2 wherein said first denomination identifier and said first serial number identifier are encrypted with a second encryption.

4. An electronic currency unit as claimed 2, wherein said first encryption is a two key encryption method.

5. A method for issuing electronic currency comprising the steps of:

generating an electronic currency unit;

assigning said electronic currency unit a value;

recording said assigned value;

issuing said electronic currency unit.

6. The method for issuing electronic currency as claimed in claim 6 further comprising the steps of:

encrypting at least a portion of said electronic currency unit.

7. The method for issuing electronic currency as claimed in claim 6 further comprising the steps of:

transmitting encryption data to an electronic currency unit storage device.

8. A system for managing electronic currency comprising;

an issuing module;

a network module; and

a redemption module.

9. An electronic currency storage device comprising;

an input port;

a memory;

a processor.

FIG-1

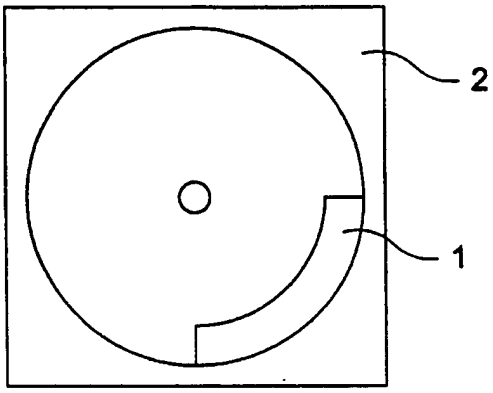

2
1

FIG-2

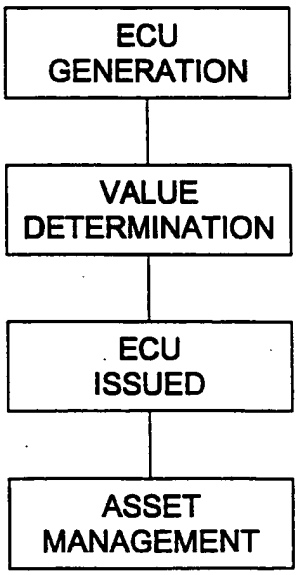

ECU GENERATION
VALUE DETERMINATION
ECU ISSUED
ASSET MANAGEMENT

FIG-3

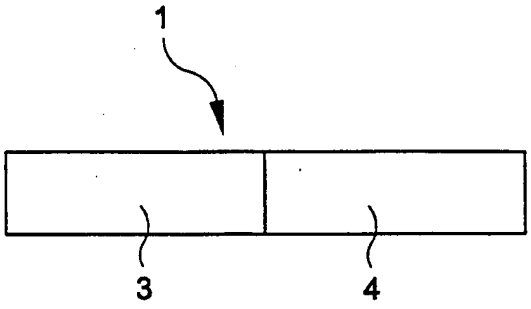

1
3
4

FIG-4

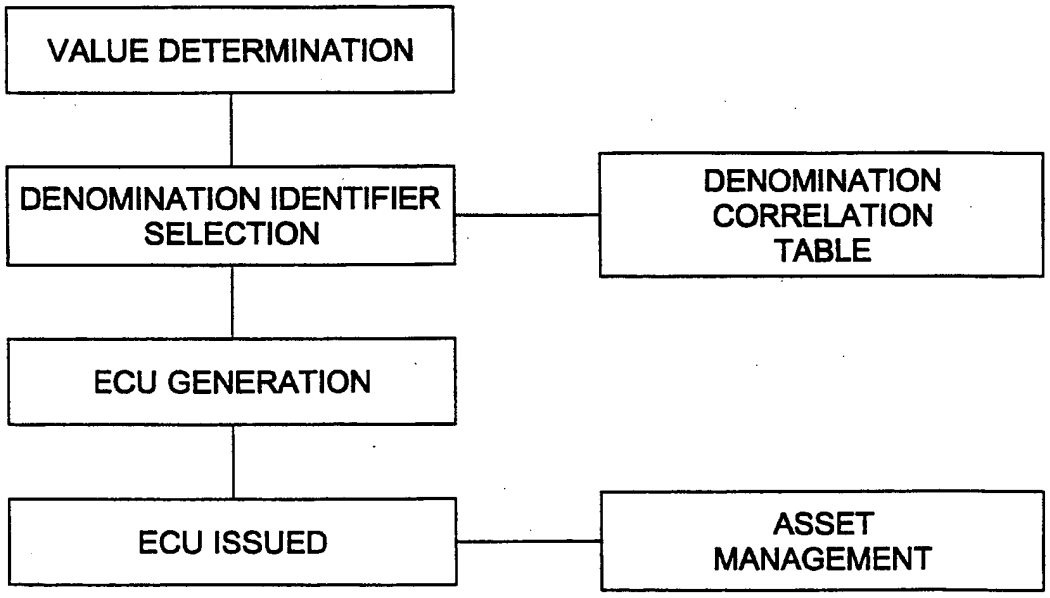

VALUE DETERMINATION
DENOMINATION IDENTIFIER SELECTION
DENOMINATION CORRELATION TABLE
ECU GENERATION
ECU ISSUED
ASSET MANAGEMENT

FIG-5

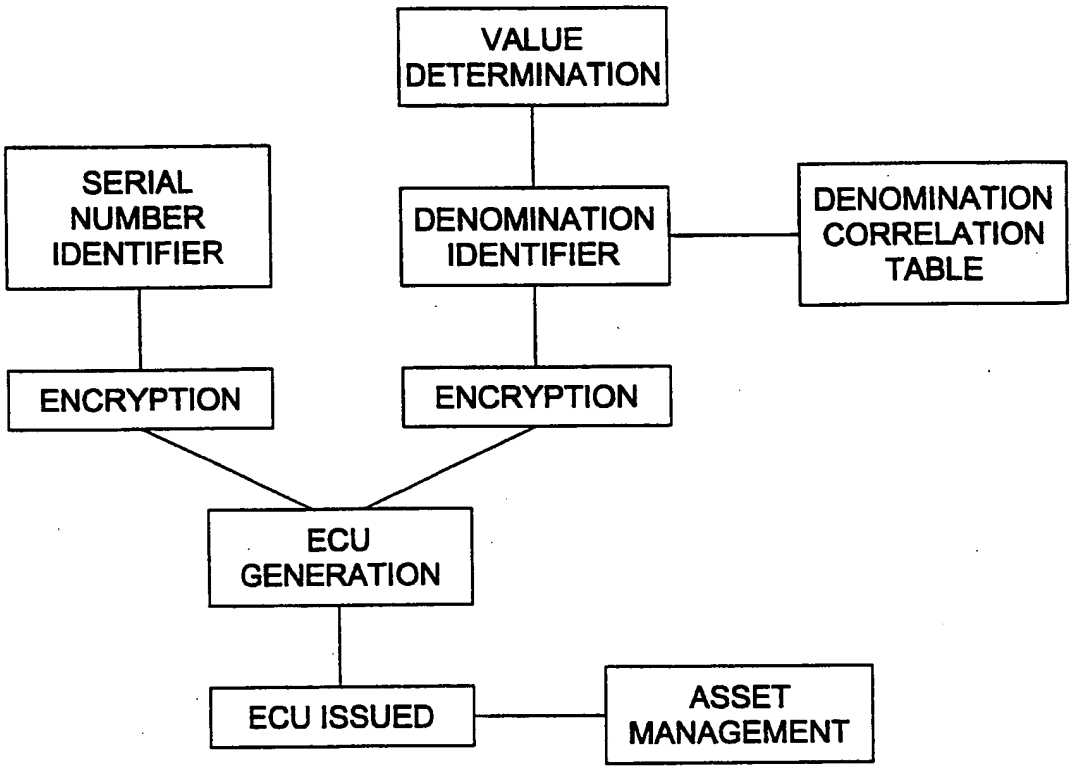

VALUE DETERMINATION
SERIAL NUMBER IDENTIFIER
DENOMINATION IDENTIFIER
DENOMINATION CORRELATION TABLE
ENCRYPTION
ENCRYPTION
ECU GENERATION
ECU ISSUED
ASSET MANAGEMENT

FIG-6

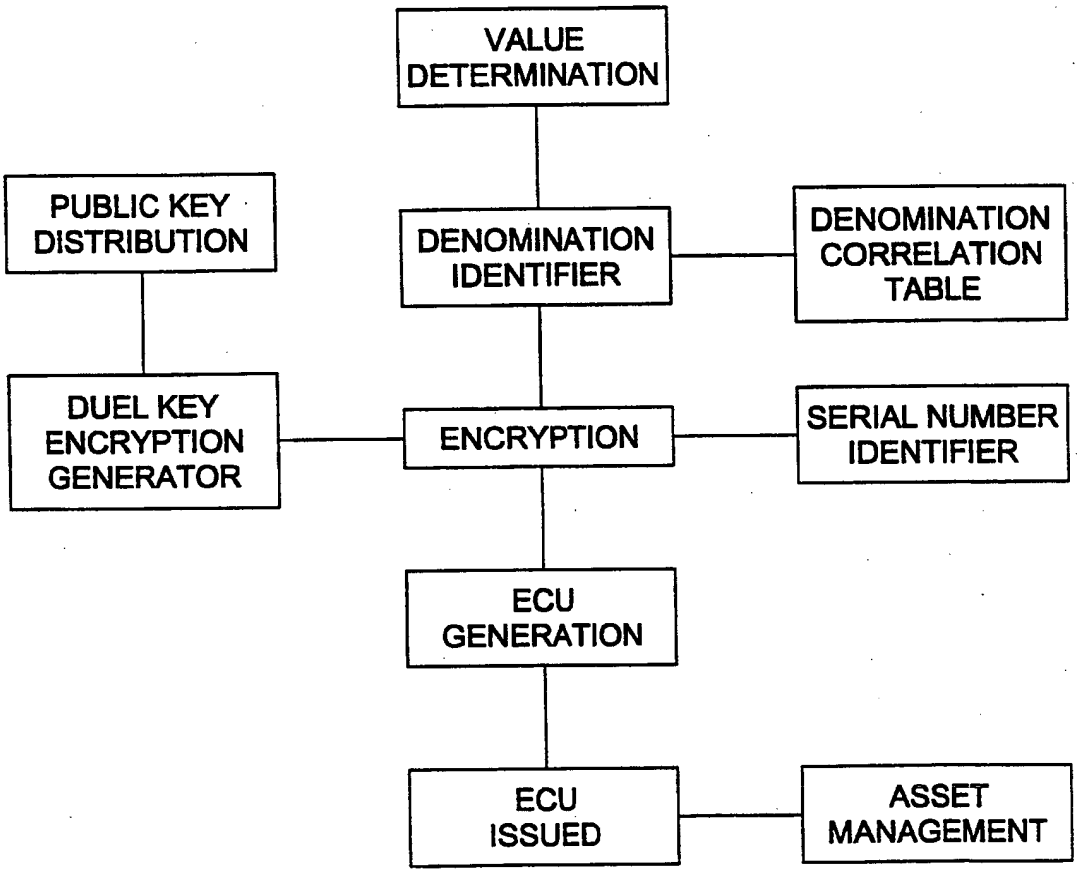

VALUE DETERMINATION
PUBLIC KEY DISTRIBUTION
DENOMINATION IDENTIFIER
DENOMINATION CORRELATION TABLE
DUEL KEY ENCRYPTION GENERATOR
ENCRYPTION
SERIAL NUMBER IDENTIFIER
ECU GENERATION
ECU ISSUED
ASSET MANAGEMENT

FIG-7

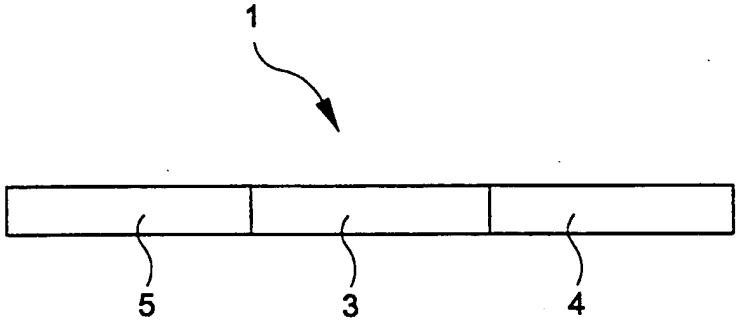


FIG-8

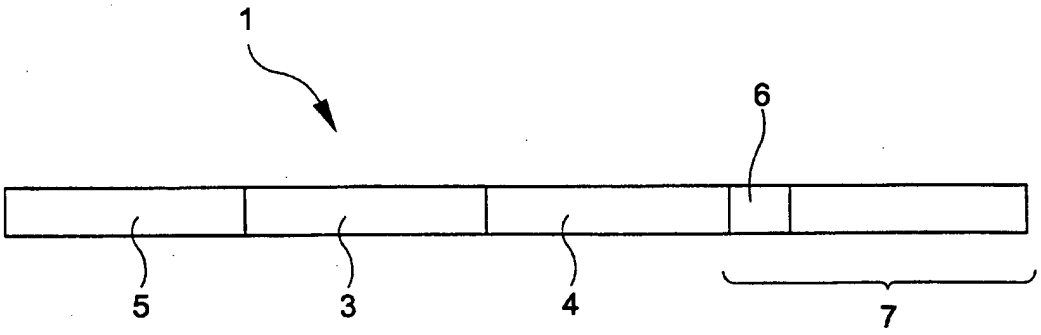


FIG-9

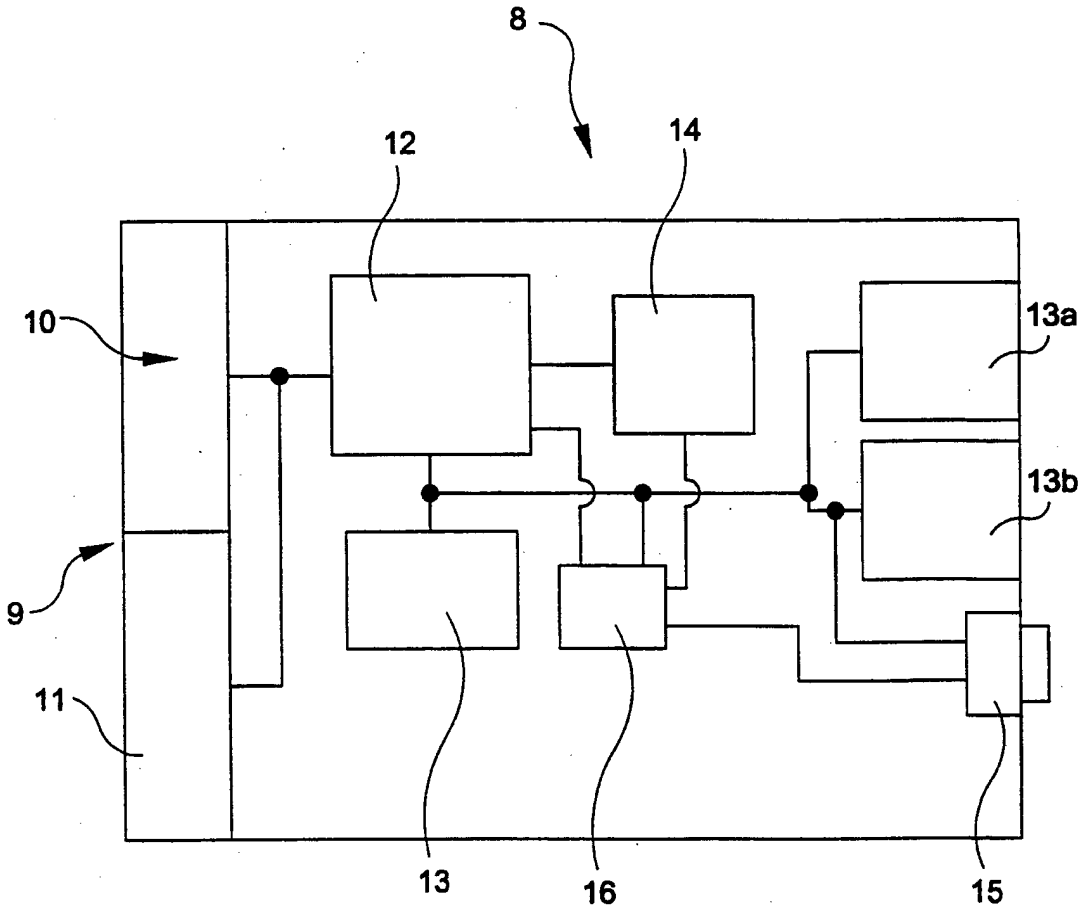


FIG-10

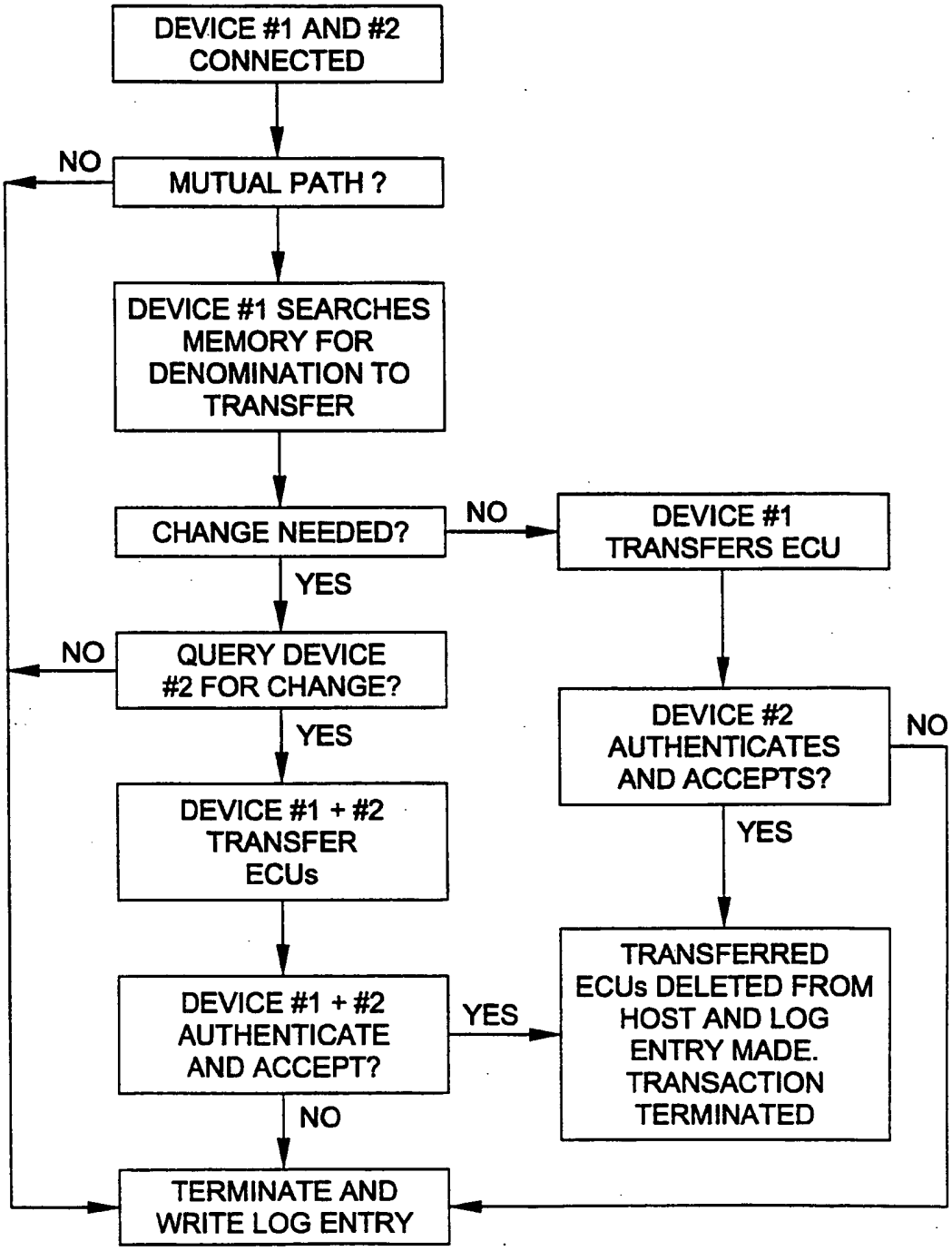

DEVICE #1 AND #2 CONNECTED
NO
MUTUAL PATH ?
DEVICE #1 SEARCHES MEMORY FOR DENOMINATION TO TRANSFER
CHANGE NEEDED?
NO
DEVICE #1 TRANSFERS ECU
YES
NO
QUERY DEVICE #2 FOR CHANGE?
DEVICE #2 AUTHENTICATES AND ACCEPTS?
NO
YES
YES
DEVICE #1 + #2 TRANSFER ECUs
TRANSFERRED ECUs DELETED FROM HOST AND LOG ENTRY MADE. TRANSACTION TERMINATED
DEVICE #1 + #2 AUTHENTICATE AND ACCEPT?
YES
NO
TERMINATE AND WRITE LOG ENTRY

FIG-11

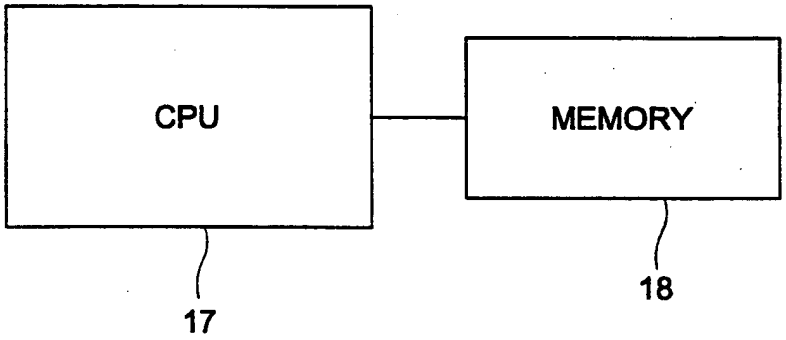
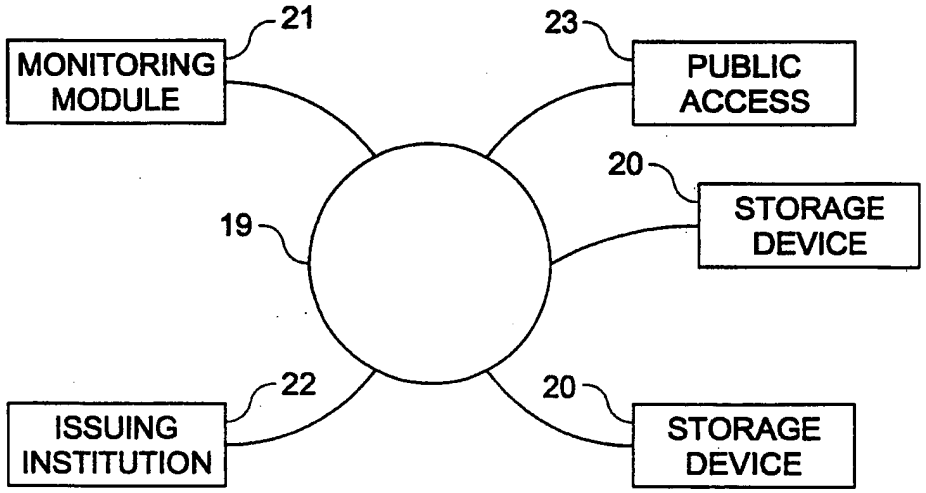

CPU
MEMORY
17
18

FIG-12


MONITORING MODULE
21
23
PUBLIC ACCESS
20
STORAGE DEVICE
19
22
ISSUING INSTITUTION
20
STORAGE DEVICE

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/60

A3

(11) International Publication Number: WO 00/10068

(43) International Publication Date: 24 February 2000 (24.02.00)

(21) International Application Number: PCT/US99/18356

(22) International Filing Date: 12 August 1999 (12.08.99)

(30) Priority Data:
09/133,824 13 August 1998 (13.08.98) US

(71)(72) Applicant and Inventor: FUISZ, Richard, C. [US/US]; 14555 Avion at Lakeside, Chantilly, VA 20151 (US).

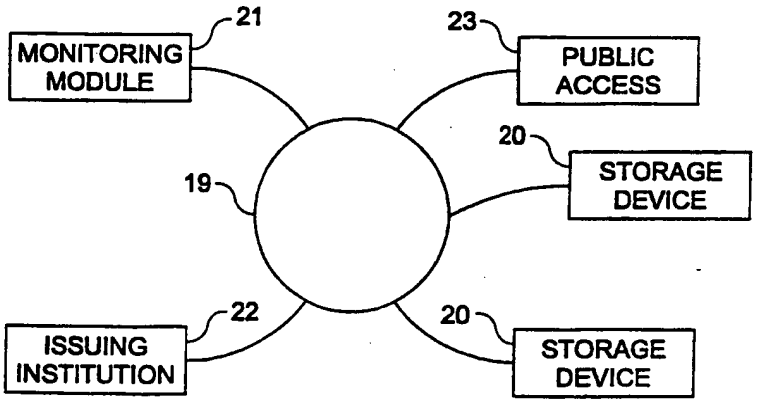
(74) Agent: BODNER, Gerald, T.; Hoffmann & Baron, LLP, 6900 Jericho Turnpike, Syosset, NY 11791 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(88) Date of publication of the international search report:
18 May 2000 (18.05.00)

(54) Title: APPARATUS FOR AND METHOD OF ELECTRONIC CURRENCY GENERATION, TRANSFER AND REDEMPTION



(57) Abstract

An electronic form of commerce that provides acceptable levels of security while at the same time permitting anonymous electronic transfers of money substitutes, including a new form of electronic currency (3 & 4), new forms of electronic counterfeit protection, a new storage device (20) that may, but which does not have to be, used with this new form of electronic currency (3 & 4), an electronic currency generator (17 & 18) and an apparatus for tracking incoming cash reserves (21).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/18356

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 17/60
US CL :705/76, 41, 40, 69, 65; 235/379

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/76, 41, 40, 69, 65; 235/379

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS and EAST: electronic currency; electronic money; encryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,754,654 A (HIROYA et al) 19 May 1998, col. 9, lines (ll.) 49-55; col. 11, ll. 58-60; col. 14, ll. 64-67; col. 15, ll. 1-10; col. 17, ll. 57-65; col. 4, ll. 28-36; col. 14, ll. 46-63; col. 16, ll. 35-49; col. 16, ll. 38-40; col. 4, ll. 49-53; col. 4, ll. 63-67; col. 3, ll. 43-67; col. 4, ll. 1-23; FIG. 1; FIG. 2; FIG. 3; FIG. 4; FIG. 5; FIG. 7; and FIG. 11.	1-9
Y	US 5,590,038 A (PITRODA) 31 December 1996, col. 2, ll. 44-67.	1-9
Y	US 5,644,727 A (ATKINS) 01 July 1997, col. 7, ll. 19-30; col. 9, ll. 25-50; and col. 10, ll. 46-48.	1-9

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
24 JANUARY 2000	14 FEB 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JOHN L. YOUNG James R. Matthews Telephone No. (703) 305-3801

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/18356

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,557,518 A (ROSEN) 17 September 1996, col. 1, ll. 65-67; col. 2, ll. 12-37.	1-9
Y	US 5,455,407 A (ROSEN) 03 Ocotber 1995, col. 1, ll. 7-17; col. 2, ll. 5-16; col. 3, ll. 39-67; col. 4, ll. 1-67; col. 5, ll. 1-44.	1-9
Y	US 5,453,601 A (ROSEN) 26 September 1995, col. 1, ll. 7-17; col. 2, ll. 5-16; cl. 3, ll. 39-67; col. 4, ll. 1-67; and col. 5, ll. 1-44.	1-9
Y,P	US 5,898,154 A (ROSEN) 27 April 1999, col. 1, ll. 7-17; col. 2, ll. 5-16; col. 3, ll. 39-67; col. 4, ll. 1-67; and col. 5, ll. 1-44.	1-9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/18356

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 6 & 7
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/60 | A3

(11) International Publication Number: **WO 00/10068**

(43) International Publication Date: 24 February 2000 (24.02.00)

(21) International Application Number: PCT/US99/18356

(22) International Filing Date: 12 August 1999 (12.08.99)

(30) Priority Data:
09/133,824 13 August 1998 (13.08.98) US

(71)(72) Applicant and Inventor: FUISZ, Richard, C. [US/US]; 14555 Avion at Lakeside, Chantilly, VA 20151 (US).

(74) Agent: BODNER, Gerald, T.; Hoffmann & Baron, LLP, 6900 Jericho Turnpike, Syosset, NY 11791 (US).

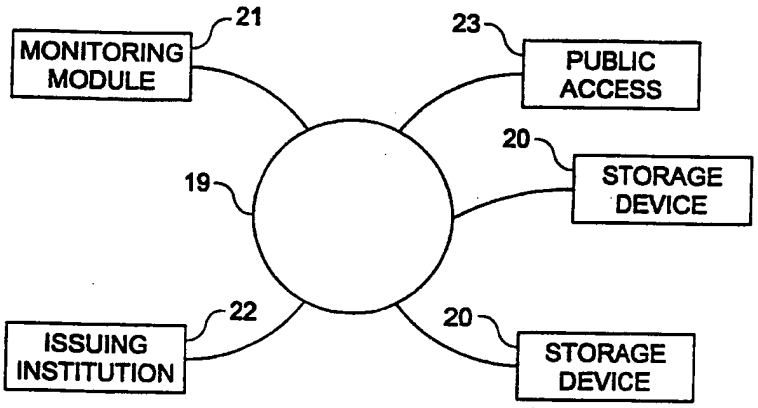
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
With amended claims.

(88) Date of publication of the international search report:
18 May 2000 (18.05.00)

Date of publication of the amended claims:
22 June 2000 (22.06.00)

(54) Title: APPARATUS FOR AND METHOD OF ELECTRONIC CURRENCY GENERATION, TRANSFER AND REDEMPTION



(57) Abstract

An electronic form of commerce that provides acceptable levels of security while at the same time permitting anonymous electronic transfers of money substitutes, including a new form of electronic currency (3 & 4), new forms of electronic counterfeit protection, a new storage device (20) that may, but which does not have to be, used with this new form of electronic currency (3 & 4), an electronic currency generator (17 & 18) and an apparatus for tracking incoming cash reserves (21).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

AMENDED CLAIMS

[received by the International Bureau on 9 March 2000 (09.03.00);
Original claim 6 amended; remaining claims unchanged (1 page)]

6. The method for issuing electronic currency as claimed in claim 5 further comprising the steps of:

encrypting at least a portion of said electronic currency unit.

7. The method for issuing electronic currency a claimed in claim 6 further comprising the steps of:

transmitting encryption data to an electronic currency unit storage device.

8. A system for managing electronic currency comprising;

an issuing module;

a network module; and

a redemption module.

9. An electronic currency storage device comprising;

an input port;

a memory;

a processor.